Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1.   (Currently Amended)   A communication device, comprising:

an executing unit configured to execute ~~means for executing~~ software;

a memory configured to store permission data, the ~~storing means for storing~~ permission data indicating permissible behavior for an application, the application being ~~which is~~ a group of functions provided by execution of the software;

a checking unit configured to check ~~means for checking~~, by accessing an external device before the software is executed, whether the permission data are valid; and

an execution control unit configured to permit the ~~means for permitting said~~ executing unit ~~means~~ to execute the software when, on the basis of a result of the check carried out by the ~~said~~ checking unit ~~means~~, the permission data are determined to be valid, and for not permitting the ~~said~~ executing unit ~~means~~ to execute the software when, on the basis of the result of the check executed by the ~~said~~ checking unit ~~means~~, the permission data are determined to be invalid.

2.   (Currently Amended)   A communication device according to claim 1, further comprising, ~~wherein,~~

~~said communication device further comprises~~ a determining unit configured to determine ~~means for determining~~ whether it is necessary to carry out the check by the ~~said~~ checking unit ~~means~~, the checking unit ~~said determining means~~ either carrying out or not carrying out the check on the basis of a determination made by the determining unit ~~said determination means~~.

3.   (Currently Amended)   A communication device according to claim 2, wherein,

the ~~said~~ determining unit ~~means~~ comprises:

a counting <u>unit configured to count</u> ~~means for counting~~ a number of executions of the software; and

a frequency data <u>memory configured to store</u> ~~storing means for storing~~ frequency data indicating how frequently it is necessary to carry out the check; and wherein,

the ~~said~~ determining <u>unit is configured to determine,</u> ~~means determines,~~ on the basis of a number of executions of the software, as counted by the ~~said~~ counting <u>unit,</u> ~~means,~~ and on the basis of the frequency data stored in the ~~said~~ frequency data <u>memory,</u> ~~storing means,~~ whether it is necessary to carry out a check by the ~~said~~ checking <u>unit</u> ~~means~~.

4. (Currently Amended) A communication device according to claim 2, wherein,

the ~~said~~ determining <u>unit</u> ~~means~~ comprises:

a timer <u>configured to provide</u> ~~means for providing~~ time data indicating a present time; and

a time interval data <u>memory</u> ~~storing means~~ for storing time interval data indicating a time interval at which it is necessary to carry out the check; and wherein,

the ~~said~~ determining <u>unit is configured to calculate</u> ~~means calculates,~~ on the basis of time data provided by the ~~said~~ timer, a time period between a present time and a time recorded at a most recent execution of the software, and determines whether it is necessary to carry out the check by the ~~said~~ checking <u>unit</u> ~~means~~ on the basis of the calculated time period and the time interval data stored in said time interval data <u>memory</u> ~~storing means~~.

5. (Currently Amended) A communication device according to claim 1, <u>further comprising:</u> ~~wherein:~~

~~said communication device further comprises~~ <u>a</u> count data <u>memory configured to store</u> ~~storing means for storing~~ count data indicating a <u>number</u> ~~count~~ of times that the software is allowed to be executed in a condition that the ~~said~~ checking <u>unit</u> ~~means~~ is unable to make the check; and

the ~~said~~ execution control <u>unit is configured to permit the</u> ~~means permits said~~ executing <u>unit</u> ~~means~~ to execute the software in a condition that the ~~said~~ checking <u>unit</u>

~~means~~ is unable to make the check up to a number of times which is indicated by the count data stored in the ~~said~~ count data memory ~~storing means~~.

6.   (Currently Amended)   A communication device according to claim 1, further comprising:

an updating unit configured to obtain ~~means for obtaining~~ update data from the ~~said~~ external device, and updating the permission data stored in the memory ~~said permission data storing means~~ on the basis of the update data.

7.   (Currently Amended)   A communication device according to claim 6, wherein:

the ~~said~~ updating unit is configured to:[[means]]

transmit[[s]], to the ~~said~~ external device, update timing data indicating a timing of a most recent update of the permission data stored in the memory, ~~said permission data storing means,~~ when the ~~said~~ checking unit ~~means~~ makes the check;

receive[[s]] update data transmitted from the ~~said~~ external device in response to the transmission of the update timing data; and

update[[s]] the permission data stored in the memory ~~said permission data storing means~~ on the basis of the update data.

8.   (Currently Amended)   A communication device according to claim 1, further comprising:

a terminating unit configured to instruct the ~~means for instructing said~~ executing unit ~~means~~ to terminate execution of the software when the application attempts to conduct behavior which the application is not permitted to conduct.

9.   (Currently Amended)   A communication device according to claim 1, wherein:

the permission data contain information on usage of at least one of an internal hardware resource of the ~~said~~ communication device, an external hardware resource of the ~~said~~ communication device, a software resource and a communication network resource.

10. (Currently Amended) A method for controlling a communication device, the method comprising:

a step for transmitting to the said communication device permission data, the permission data indicating which indicates permissible behavior for an application, the application being which is a group of functions provided by execution of software in the said communication device;

a step for checking, by communicating data between the said communication device and an external device, whether the permission data are valid, before the software is executed in the said communication device; and

a step for permitting the software to be executed only when the permission data are determined to be valid on the basis of a result of the check.

11. (Currently Amended) A computer readable storage medium storing a program for causing instructing a computer to execute a process, the process comprising:

a process for storing, in a memory storing means, permission data indicating permissible behavior for an application, the application being which is a group of functions provided by execution of software;

a process for checking, by accessing an external device, whether the permission data are valid, before the software is executed; and

a process for permitting the software to be executed only when the permission data are determined to be valid on the basis of a result of the check.

12. (Currently Amended) A communication method comprising: a step for transmitting from in a communication system comprising (a) a software data providing server device which stores software data containing software for providing a group of functions forming an application, (b) a management server device which stores security descriptor data containing permission data indicating permissible behavior for the application, and (c) an application descriptor data providing server device which stores

application descriptor data indicating a storage location of the software data and a storage location of the security descriptor data, ~~to said communication device the application descriptor data;~~ the method comprising:

~~a step for~~ transmitting the application descriptor data from said communication system to said communication device;

~~a step for~~ transmitting data indicating the storage location of the security descriptor data contained in the application descriptor data from said communication device to said communication system;

~~a step for~~ transmitting the security descriptor data from said communication system to said communication device on the basis of the data indicating the storage location of the security descriptor data;

~~a step for~~ storing the security descriptor data in said communication device;

~~a step for~~ transmitting data indicating the storage location of the software data contained in the security descriptor data from said communication device to said communication system;

~~a step for~~ transmitting the software data from said communication system to said communication device on the basis of the data indicating the storage location of the software data;

~~a step for~~ installing, in said communication device, the software contained in the software data transmitted from said communication system to said communication device;

~~a step for~~ checking, by communicating data between said communication device and said communication system before the software is executed in said communication device, whether the security descriptor data stored in said communication device are valid; and

~~a step for~~ permitting said software to be executed in said communication device only when the security descriptor data are determined to be valid on the basis of a result of the check.

13.   (New)   A communication device according to claim 1, wherein the application comprises a Java application; and

wherein the permission data comprises a scope of rights which are granted to the Java application.

14. (New) A communication device according to claim 1, wherein the permission data indicates that the application is allowed to access information designated as confidential.

15. (New) A communication device according to claim 1, wherein the permission data indicates that the application is allowed to access telephone directory information.

16. (New) A communication device according to claim 1, wherein permission data indicates that the application is allowed to access e-mail information.

17. (New) A communication device according to claim 1, wherein permission data indicates that the application is allowed to reconfigure the communication device.

18. (New) A communication device according to claim 1, wherein permission data indicates that the application is allowed to access configuration information relating to the communication device.

19. (New) The method according to claim 10, wherein the permission data indicates that the application is allowed to access information designated as confidential.

20. (New) The computer readable storage medium according to claim 11, wherein the permission data indicates that the application is allowed to access information designated as confidential.

21. (New) The method according to claim 12, wherein the permission data indicates that the application is allowed to access information designated as confidential.